439

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 2/19/1998

To: Director, FBI Attn: Acting Unit Chief

From: WFO
C-17/NVRA
Contact: SSA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :rar

File Number(s): 288-HQ-1242560 99 (Pending)

Title: SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ

Synopsis: Following is the status of WFO's involvement in this investigation as of 2/19/98.

Reference: EC dated 2/17/98 to Houston Division.

Details:

288-WF-211047 "[redacted] U.S. NAVY - VICTIM; OO: WFO".

SA [redacted] is coordinating all investigative activity with Agents of the Naval Criminal Investigative Service (NCIS) based in both Washington, D.C. and Jacksonville, Florida. Evidence obtained from subject's University of Northern Florida (UNF) account has disclosed continuing access to that account from an IBM.NET connection. The Trap & Trace/pen register order for [redacted] is being submitted this evening to the magistrate. Order requires [redacted] Results are anticipated to support a subsequent 2703 (d) order to [redacted] for [redacted] The subject's current whereabouts and employment are known. Coordination with the NCIS Agents will continue. The installation of the monitoring software at [redacted] was initiated [redacted] by [redacted] WFO is contacting Georgetown University, University of Virginia, and b3 b6 b7C

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995

Georgia State University, and the original ISP victim/complainant in Lawton, OK.

288-HQ-1242560 "SOLAR SUNRISE: CITAC MATTERS: OO: HQ"

Optical disks received from Houston. Copies will be made ASAP for AF, Navy, DISA, and [redacted] Contact has been made with IBM network management and IBM is trace routing Israeli network leg. Should know soon of monitoring ability from within US of overseas leased nets. Referral/Consult

Analysis performed for three compromised systems: (1) Univ. California, Berkeley, (2) Andrews AFB, (3) US Naval Academy. To date, nothing significant has been identified in the most recent JID data collected for the past day or so. Observed two suspicious sites (netgate.saes.com and netdex.com). WFO has not confirmed the nexus on these sites.

Gospelcom.net not contacted due to NCIC checks revealing [redacted] Thegospel.com does not answer phone, nor do they call back when message left. Will continue to try to contact. Slip-stream.net SYSOP did not see anything unusual. They have been hacked before and do not consider this out of the norm b6 b7C b3 OTHER Sealed pursuant to court order

On 02/13/98, Court Order served on [redacted] Second 2703 (b) order provided to [redacted] Second order will provide additional information.

FERMI Labs and Oakridge National Labs report no intrusions at their sites. All traffic to/from labs is legitimate and explainable. No known connection to this case.

No further information from DISA.

288-WF-NEW [redacted] VICTIM; OO: WFO"

SA [redacted] is addressing this matter with the assistance of the [redacted] and WFO CART. Subject's home was consensually searched for computer and computer media the evening of 2/17/98. Newark Division CART [redacted] Copy will be provided b6 b7C b7E Referral/Consult

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

To: WMFO From: WMFO
Re: 66-, 12/01/1995 Referral/Consult

to [redacted] ASAP. Subject provided detailed interview to both FBI and [redacted] Agents. Gave no indication he was part of ongoing investigation 288-HQ-1242560. A review of his system is under way.